IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

SYSTEM ONE HOLDINGS, L.L.C., a	)	
Delaware limited liability company,	)	
	)	
Plaintiff	)	
	)	
v.	)	02: 07cv0132
	)	
RALPH H. HILL, JR., an individual and	)	
DIAMOND TECHNICAL SERVICES, INC.,	)	
a Pennsylvania corporation,	)	
	)	
Defendants.	)	

STIPULATED PROTOCOL FOR THE HANDLING AND ANALYSIS OF COMPUTER DATA

Plaintiff, System One Holdings, L.L.C. (referred to for purposes of this Protocol as "Hudson"), and Defendants, Ralph H. Hill, Jr. ("Hill"), and Diamond Technical Services, Inc. ("Diamond") (Plaintiffs and Defendants are collectively referred to herein as the "Parties"), have stipulated to, and this Court hereby enters, the following Stipulated Protocol for the Handling and Analysis of Computer Data.

The following methodology shall be used by the Parties in substantively analyzing the contents of the 80 gigabyte Western Digital external hard drive (the "External HD") and home personal computer hard drive (the "Home HD") that were delivered into the Court's custody by Hill on or about February 13, 2007 (collectively the "Target Devices") by means of bitstream images of the Target Devices generated pursuant to the Parties' October 18, 2007 Stipulated Protocol for the Acquisition of Computer Data (the "Acquisition Protocol").

I. Background and Objectives

A. On October 18 and 19, 2007, pursuant to the Acquisition Protocol, Cyber Controls, LLC (Hill's and Diamond's computer forensics expert) generated bitstream images of the Target Devices (the "Copied Images"). The generation of the Copied Images was observed by counsel for each of the Parties, along with a representative of JurInnov, Ltd. (Hudson's computer forensics expert). Cyber Controls, LLC prepared two separate external hard drives, each of which contains identical versions of the Copied Images. The Parties have agreed that the Copied Images are identical to the contents of the Target Devices. The Copied Images have been delivered to the Court's custody along with the Target Devices.

B. The Parties wish to establish a method by which Hudson and Hill may analyze the contents of the Copied Images for use in the above-captioned proceeding (the "Litigation").

C. Hill has asserted that the Copied Images may contain certain Personal Information (as defined herein), Privileged Information (as defined herein), and/or Known System Files (as defined herein) and that the revelation of such Personal Information, Privileged Information or Known System Files to Hudson and/or to Diamond, even subject to the Stipulated Protective Order entered on October 19, 2007 (the "Protective Order"), would be both damaging to Hill and unnecessary and irrelevant to the Litigation.

1. For purposes of this Protocol, the term "Personal Information" shall mean information that meets all of the following criteria: (i) the information is private and/or personal to Hill or to Hill's family members; and (ii) the information has no relevance whatsoever to any of the claims or defenses asserted or substantive positions taken by any of the Parties in connection with the Litigation.

2. For purposes of this Protocol, the term "Privileged Information" shall mean information that constitutes or reflects communications between Hill and his legal counsel for the purpose of obtaining legal advice on any matters, including, but not limited to,

the Litigation. The term "Privileged Information" shall also include any work product prepared by Hill's legal counsel as a result of communications between them. The term "Privileged Information" shall not include materials prepared by individuals other than Hill's legal counsel for purposes related to legal matters, including the Litigation, unless the materials in question would reveal the substance of otherwise protected communications.

3. For purposes of this Protocol, the term "Known System Files" shall mean those standard computer files necessary for the operation of a computer's operating system, software or programs installed on a computer, images or graphics commonly installed on a computer, and/or other files not commonly accessed directly by the end user of a computer. Such files can be identified using the MD5 hash values commonly available for download from the National Software Reference Library, as maintained by the National Institute of Standards and Technology (www.nsrl.nist.gov).

D. This Protocol will be performed in compliance with the terms of the Court's May 25, 2007 Order, which precludes Hill from using or disclosing any of Hudson's information or materials in any manner. Hill agrees that neither he nor anyone acting on his behalf (including Hill's counsel and/or Cyber Controls, LLC) will directly or indirectly furnish or disclose any such information or materials to Diamond (or any of Diamond's officers, agents, representatives, or employees, other than to Diamond's counsel in this Litigation as described in Sections III and IV of this Protocol), or to any other third-parties at any point during or after performance of this Protocol without first obtaining Hudson's express written consent.

II. Identification of Active Files Containing Personal Information, Privileged Information and/or Known System Files

A. Pursuant to this Protocol, Hill's undersigned counsel may obtain one of the two external hard drives containing the Copied Images from the Court's custody.

B. Pursuant to this Protocol, Hudson's counsel (assisted by JurInnov, Ltd.), Hill's counsel, Mr. Hill, and Cyber Controls, LLC, will conduct a joint inspection of the Copied Images contained on the external hard drive that has been obtained from the Court's custody in order to identify those files contained within the active / allocated sectors of the Copied Images that constitute Personal Information, Privileged Information and/or Known System Files on each of the Target Devices (the "Joint Inspection"). Neither Hudson nor Diamond, nor any of their respective officers, agents, representatives or employees, will directly participate in the Joint Inspection.

C. During the Joint Inspection, Hill's counsel and Hudson's counsel will cooperate in good faith to resolve any disagreements as to the status of materials as Personal Information, Privileged Information and/or Known System Files. Any disputes that cannot be resolved between counsel will be promptly submitted to the Court for a decision.

D. This Protocol will be performed separately with regard to each of the Target Devices, and unless otherwise noted herein, the Protocol will be performed in the same manner as to each of the Target Devices.

E. For each of the Target Devices, Cyber Controls, LLC will generate a list identifying all materials that are determined (either by agreement or by Court decision) during the Joint Inspection to be Personal Information and/or Privileged Information (the "Exclusion List – Home HD" and the "Exclusion List – External HD"). For the Target Device representing

Hill's home personal computer, Cyber Controls will also generate a list identifying all materials that are determined (either by agreement or by Court decision) to be Known System Files (the "Known System Files Exclusion List – Home HD"). The Exclusion Lists will include the following details for each identified file: the name of the file; the location or path of the file (including the piece of equipment on which the file is housed); the MD5 hash value of the file; the logical size of the file, and any other identifying information that is generated by EnCase during the Joint Inspection. The Exclusion Lists will be provided to the Parties' counsel in Microsoft Excel format at the end of the Joint Inspection.

F. Following the Joint Inspection, Hill's counsel will generate a privilege log as to any files that Hill contends constitute Privileged Information and will provide this privilege log to Hudson's counsel and Diamond's counsel.

III. **Production and Review of Secondary Images of Active / Allocated Space**

A. Using the Exclusion Lists, Cyber Controls, LLC will generate secondary images of the active / allocated sectors of each of the Target Devices, excluding from the secondary images only those files that appear on the Exclusion Lists. The secondary images will be created by Cyber Controls, LLC from the external hard drive containing the Copied Images in accordance with the following process for each of the applicable Exclusion Lists:

1. The MD5 hash values of the files that appear on the Exclusion List will be generated by EnCase.

2. A hash set called "Excluded Files" will be created using EnCase for the Exclusion List. This hash set will include all of the files that appear on the Exclusion List.

3. The "Excluded Files" hash set will be imported into the EnCase Hash Library of the external hard drive containing the Copied Images and the EnCase Hash Library of the external hard drive containing the Copied Images will be rebuilt.

4. All files on the drive containing the Copied Images will be re-hashed.

5. An EnCase Logical Evidence File (file extension ".L01") will be created for each of the Target Devices (the "Active EnCase File – Home HD" and the "Active EnCase File – External HD").

6. Any files contained within the "Excluded Files" hash set will be excluded from the Active EnCase File.

7. The Active EnCase Files will contain all of the files originally contained in the active / allocated sectors of the respective Target Devices, with the exception of the files contained within the "Excluded Files" hash sets.

B. Cyber Controls, LLC will provide each of the Active EnCase Files, along with the applicable Exclusion Lists, to Hudson's counsel, to Hill's counsel, and to Diamond's counsel at the end of the Joint Inspection.

C. Upon receipt of the Active EnCase Files and Exclusion Lists, Hudson's counsel may share these materials with Hudson and with JurInnov, Ltd., and Hudson may use the files and materials contained therein for any purpose in the Litigation.

D. Upon receipt of the Active EnCase Files and Exclusion Lists, Hill's counsel may share these materials with Cyber Controls, LLC for any purpose in the Litigation. Hill may review these materials only in the presence of Hill's counsel, and Hill may not take possession of any of these materials or their contents, either in print or electronic form. Hill's review of these materials will be performed in compliance with the terms of the Court's May 25, 2007 Order, as described in Section I(D) of this Protocol.

E. Upon receipt of the Active EnCase Files and Exclusion Lists, Diamond's counsel may review these materials on an "Attorneys' Eyes Only" basis, but may not share these materials with Diamond or any of its officers, agents, representatives or employees.

F. Hudson's counsel, Hill's counsel, and Diamond's counsel may retain possession of the Active EnCase Files and related Exclusion Lists for the duration of the Litigation.

IV. Production and Review of Non-Active / Unallocated Space

A. During the Joint Inspection, Cyber Controls, LLC will generate an EnCase Logical Evidence File for each of the Target Devices that includes the following files, data, and information from each of the Target Devices (the "Non-Active EnCase File – Home HD" and the "Non-Active EnCase File – External HD"):

1. an image of the entire non-active / unallocated space (including all applicable sectors) from the Target Device;

2. all temporary internet files contained on the Target Device;

3. all files entitled "pagefile.sys" and/or "hyberfil.sys;" and

4. complete images of all Registries that are housed on the Target Device (including NTUSER.dat and all software and/or system registry files).

B. Cyber Controls, LLC will provide the Non-Active EnCase Files to Hudson's counsel, to Hill's counsel, and to Diamond's counsel at the end of the Joint Inspection.

C. Upon receipt of the Non-Active EnCase Files, Hudson's counsel, with the assistance of JurInnov, Ltd, may review the contents of these files as it sees fit, subject only to the following process by which Hill may designate certain materials as Personal Information and/or Privileged Information:

1. Initially, Hudson's counsel may provide JurInnov, Ltd. with any number of separate requests for portions of the Non-Active EnCase Files. These requests may be in the form of search parameters (e.g., for the non-active / unallocated space) or requests for specific segments of the Target Devices (e.g., a request for the entire NTUSER.dat registry). Hudson's initial requests for portions of the Non-Active EnCase Files will be submitted to JurInnov, Ltd., in one set.

2. The results generated by JurInnov, Ltd. in response to Hudson's counsel's initial set of requests will be provided to Hill's counsel and to Hudson's counsel either on a compact disc or by means of a secure internet website.

3. In performing searches within the Non-Active EnCase Files pursuant to search parameters provided by Hudson's counsel, JurInnov, Ltd. will generate a hit report for each search parameter. Each hit contained in a hit report will be separately numbered and, for any searches performed within the non-active / unallocated space, will include a unique file offset reflecting that hit's position within the unallocated space.

4. Upon receipt of the results of Hudson's counsel's initial set of requests, Hill's counsel may review those results for the purpose of identifying and designating Personal Information and/or Privileged Information contained therein. Hill's counsel will provide Hudson's counsel with a list of any items or data that it contends constitute Personal Information or Privileged Information, identifying for each such item: (i) the location of the item with a particular result; (ii) the number assigned to the item (in the case of hit reports generated from searches of the non-active / unallocated space); (iii) the portion of the item that

constitutes Personal Information or Privileged Information; and (iv) an explanation of the basis for designating the content as Personal Information or Privileged Information. Hill's counsel will provide these lists to Hudson's counsel by the end of the third business day following Hill's counsel's receipt of the results. If Hill's counsel fails to provide its aforementioned designations of Personal Information and Privileged Information to Hudson's counsel within this time period (or such other time period as may be agreed upon between counsel), the results in question will be deemed to contain no Personal Information or Privileged Information.

5. To the extent that Hill's counsel designates the contents of any results as Personal Information and/or Privileged Information, Hill's counsel and Hudson's counsel will cooperate in good faith to resolve any disagreements as to such designations. In this regard, Hill's counsel and Hudson's counsel will take into consideration the significance of the alleged Personal or Privileged Information and the harm that would result from its revelation for purposes of the Litigation subject only to the Protective Order, particularly in light of Section VI of this Protocol below. Any disputes that cannot be resolved between counsel will be promptly submitted to the Court for a decision.

6. Any portions of results that are determined (either by agreement or by Court decision) to constitute Personal and/or Privileged Information will be redacted from JurInnov, Ltd.'s work product prior to being shared with Hudson or offered as evidence at trial.

7. Once a set of results has been subjected to this review process and redacted as necessary to remove designated Personal and/or Privileged Information, Hudson's counsel (i) may share those results with Hudson; (ii) may use those results for any purpose in the Litigation; and (iii) may provide JurInnov, Ltd. with additional sets of requests, each of which shall be subject to this review process.

8. Subject to extension by agreement or Court Order, Hudson shall complete its searches pursuant to this Section IV(C) within 90 days from the filing of this Protocol.

D. Upon receipt of the Non-Active EnCase Files, Hill's counsel may share these materials with Cyber Controls, LLC for any purpose in the Litigation. Hill may review these materials only in the presence of Hill's counsel, and Hill may not take possession of any of these materials or their contents, either in print or electronic form. Hill's review of these materials will be performed in compliance with the terms of the Court's May 25, 2007 Order, as described in Section I(D) of this Protocol.

E. Upon receipt of the Non-Active EnCase Files, Diamond's counsel may review these materials on an "Attorneys' Eyes Only" basis, but may not share these materials with Diamond or any of its officers, agents, representatives or employees.

V. Identification and Review of Internet History

A. During the Joint Inspection, Cyber Controls, LLC will identify any and all "index.dat" files (i.e., files that collect and track unique URL entries reflecting a user's internet / website visit history) contained on the Home HD and will sort the URL entries contained therein by the date on which each entry was created.

B. During the Joint Inspection, Cyber Controls, LLC will generate two Microsoft Excel documents reflecting the contents of the "index.dat" files, as follows:

1. one Microsoft Excel document listing all URL entries that were either created or last written within the "index.dat" file prior to September 1, 2006, including for each URL entry any and all identifying information that is generated by EnCase during the Joint Inspection (the "Internet History Exclusion List – Home HD"); and

2. one Microsoft Excel document listing all URL entries that were either created or last written within the "index.dat" file on or after September 1, 2006, including for each URL entry any and all identifying information that is generated by EnCase during the Joint Inspection (the "Internet History Inclusion List – Home HD").

C. Cyber Controls, LLC will provide the Lists described in Section V(B) above to Hudson's counsel, to Hill's counsel, and to Diamond's counsel at the end of the Joint Inspection. These Lists shall be handled by counsel and shared with Hudson, Hill, and Diamond on the same terms as are described above with regard to the Active EnCase Files.

VI. Identification and Deletion of Hudson Information from Target Devices

A. In accordance with the Court's May 25, 2007 Order, Hudson and Hill will cooperate in good faith to identify and segregate any and all files, materials, and/or data (including metadata) that belong or pertain to Hudson or its operations from those files, materials, and/or data (including metadata) that constitute Hill's Personal Information, Privileged Information, and/or Known Systems Files, so that Hudson's materials may be returned to Hudson and permanently and completely deleted from the Target Devices and Hill's information may be returned to him, along with the Target Devices themselves.

B. Hudson and Hill agree that any files, materials, and/or data contained or reflected in the following materials generated during the Joint Inspection and pursuant to this Protocol will be presumptively deemed to be Hudson's information:

1. the Active EnCase File – Home HD;

2. the Active EnCase File – External HD; and

3. the Internet History Inclusion List – Home HD.

C. Hudson and Hill agree that any files, materials, and/or data reflected in the following materials generated during the Joint Inspection and pursuant to this Protocol will be presumptively deemed to be Hill's information:

1. the Exclusion List – Home HD;

2. the Exclusion List – External HD; and

3. the Known System Files Exclusion List – Home HD.

D. Notwithstanding the foregoing presumptions, Hudson and Hill may each review the materials that have been presumptively characterized as Hudson's or Hill's information and may identify additional materials that should be recharacterized for purposes of ultimately restoring Hudson's information to Hudson and Hill's information to Hill. Hudson and Hill will cooperate in good faith in this regard, and any disputes that cannot be resolved between Hudson and Hill will be promptly submitted to the Court for a decision.

E. Subject to Hudson's and Hill's ability to recharacterize certain materials as described above, the materials generated pursuant to this Protocol will ultimately be handled, through Hudson's and Hill's respective computer forensics experts, as follows:

1. any active or system files that are determined to belong to Hill (presumptively reflected in the Exclusion List – Home HD, the Exclusion List – External HD, and the Known System Files Exclusion List – Home HD) will be returned to Hill;

2. any active files that are determined to belong to Hudson (presumptively reflected in the Active EnCase File – Home HD and the Active EnCase File – External HD) will be returned to Hudson and removed from the Target Devices;

3. the contents of the Non-Active EnCase Files will be permanently deleted and will not be returned to either Hudson or Hill;

4. the data reflected in the Internet History Exclusion List – Home HD and the Internet History Inclusion List – Home HD (i.e., any and all "index.dat" files) will be permanently deleted and will not be returned to either Hudson or Hill; and

5. any and all non-active data resident on the Target Devices (including all non-active / unallocated space, file slack, cookies, system restoration or backup files, and thumbnail databases) will be permanently deleted and will not be returned to either Hudson or Hill.

F. The two external hard drives containing the Copied Images will be maintained in their original form for the duration of the Litigation. Cyber Controls, LLC will retain custody of the external hard drive that it obtained in connection with the performance of this Protocol, while the Court will retain custody of the other external hard drive. At the end of the Litigation, the two external hard drives containing the Copied Images will be forensically wiped by means of a process to be agreed upon between Hill's counsel and Hudson's counsel.

VII. Additional Procedures

In the event that any portion of this Protocol is inappropriate for any of the purposes described herein, accepted computer forensic procedures will be utilized by agreement of Hill's and Hudson's respective computer forensics experts.

So Stipulated,

COHEN & GRIGSBY, P.C.
/s/ Robert M. Linn
Robert M. Linn (Pa. ID No. 44777)
Eric S. Newman (Pa. ID No. 89949)
Cohen & Grigsby, P.C.
11 Stanwix Street 15th Floor
Pittsburgh, PA 15222
Phone: (412) 297-4900
Counsel for Plaintiff, SYSTEM ONE HOLDINGS, L.L.C.

MARSHALL, DENNEHY, WARNER, COLEMAN
& GOGGIN, P.C.

/s/ Stuart H. Sostmann
Stuart H. Sostmann (Pa. ID No. 84065)
Teresa O. Sirianni (Pa. ID No. 90472)

Marshall, Dennehy, Warner, Coleman & Goggin, P.C.
2900 US Steel Tower,
600 Grant Street
Pittsburgh, PA 15219
Phone: (412) 434-5544
Counsel for Defendant, RALPH H. HILL, JR.

CIPRIANI & WERNER, P.C.

/s/ Carl E. Harvison
Carl E. Harvison (Pa. ID No. 27681)
Jamie L. Lenzi (Pa. ID No. 51865)

Cipriani & Werner, P.C.
650 Washington Road, Suite 700
Pittsburgh, PA 15228
Phone: (412) 563-2500

Counsel for Defendant,
DIAMOND TECHNICAL SERVICES, INC.

SO **ORDERED** this 19th day of May, 2008.

BY THE COURT:

s/Terrence F. McVerry
United States District Court Judge

cc: All Counsel of Record